

NEW YORK UNIVERSITY

HIPAA Information Security Policies, Specifications, and Definitions

Policy 4. Workforce Security

Responsible Officer: Associate Provost and Chief Information Technology Officer
Effective Date: January 1, 2005
Compliance Deadline: April 21, 2005
Date of Latest Revision: April 15, 2005

POLICY STATEMENT

New York University strives to protect the *confidentiality, integrity, and availability* of *EPHI* by implementing reasonable and appropriate safeguards to prevent unauthorized access to *EPHI* while ensuring that properly authorized *workforce members*' access to *EPHI* is permitted. Who is affected by this policy is documented in HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation.

REASON FOR POLICY

The conduct of New York University's *workforce members* in striving to safeguard *EPHI* is integral to the University's compliance efforts under the *HIPAA Security Regulations*. This policy reflects New York University's commitment to comply with such regulations by instituting safeguards to prevent unauthorized access to *EPHI*.

OPERATIONAL REQUIREMENTS

- A. Only properly authorized *workforce members* shall have access to *EPHI* Systems. *Workforce members* shall not attempt to gain access to any *EPHI* that they are not properly authorized to access. Each *covered component* shall train its *workforce members* on proper and appropriate use of access rights.
- B. Each *covered component* shall take reasonable and appropriate steps to ensure that *workforce members* who work with or have the ability to access *EPHI* are properly authorized and/or supervised, as set forth in the *Authorization and/or Supervision operational specification* (see 4.A).
- C. New York University *workforce members* shall be screened, as appropriate, during the hiring process, as set forth in its *Workforce Clearance Procedure operational specification* (see 4.B) and local and central Human Resources procedures.
- D. Each *covered component* shall implement a documented process for terminating access to *EPHI* when employment of *workforce members* ends or when access is no longer appropriate under New York University's *Information Access Management policy* (HIPAA Policy 5) and *Access Establishment and Modification operational specification* (see 5.B), as set forth in its *Termination Procedures operational specification* (see 4.C).

E. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards
TYPE: Standard
HIPAA HEADING: Workforce Security
REFERENCE: 45 CFR 164.308(a)(3)(i)

SECURITY REGULATION STANDARDS LANGUAGE: “Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) [Information access management] of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.”

OPERATIONAL SPECIFICATIONS

4.A Authorization and/or Supervision

1. Each *covered component* will take reasonable and appropriate steps to ensure that *workforce members* who have the ability to access *EPHI* or work in areas where *EPHI* might be accessed shall be properly authorized and/or supervised. Each *covered component* of New York University will use its **Minimum Necessary Policy**, which is one of its HIPAA Privacy policies, and other policies as appropriate, as the basis for the type and extent of authorized access to *EPHI*.
2. Each *covered component* will establish a documented process for granting authorization and access to *EPHI*, including:
 - a. Procedures for granting different levels of access to *EPHI* and to areas where *EPHI* might be accessed.
 - b. Procedures for logging and tracking authorization of *workforce members*’ access to *EPHI* and to areas where *EPHI* might be accessed.
 - c. Procedures for logging and tracking authorization of third parties’ access to *EPHI* and areas where *EPHI* might be accessed.
3. *Workforce members* shall not be allowed access to *EPHI* or to areas where *EPHI* might be accessed until proper authorization is granted.
4. Only authorized New York University *workforce members* who have need for specific information in order to fulfill their respective job responsibilities shall be authorized to access *EPHI* or areas where *EPHI* might be accessed. Each *covered component*, as appropriate, shall document and review access levels on a periodic basis and make revisions as necessary. Each *covered component*, as appropriate, shall establish a procedure for reviewing and revising, on a periodic basis, authorization of access to *EPHI* or to areas where *EPHI* might be accessed.

5. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: ADDRESSABLE Implementation Specification for Workforce Security Standard

HIPAA HEADING: Authorization and/or Supervision

REFERENCE: 45 CFR 164.308(a)(3)(ii)(A)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement procedures for the authorization and/or supervision of *workforce members* who work with electronic protected health information or in locations where it might be accessed.”

4.B Workforce Clearance Procedure

1. New York University is committed to take reasonable and appropriate steps to ensure that *workforce members* have the appropriate authorization to access *EPHI*.
2. The appropriate Human Resources and hiring personnel of the *covered component* shall identify and define the security responsibilities of and supervision required for the defined organizational position. Security responsibilities include responsibilities for implementing or maintaining

security and the protection of the *confidentiality, integrity, and availability* of New York University or *covered component information systems* or processes.

3. Each *covered component* shall review prospective *workforce members'* backgrounds during the hiring process and, as appropriate, shall perform verification checks on prospective *workforce members*. Each *covered component* shall analyze prospective *workforce members'* access to and expected abilities to modify or change *EPHI* as one of the bases for the type and number of verification checks conducted. Verification checks may include:
 - a. Confirmation of claimed academic and professional experience and qualifications
 - b. Professional license validation
 - c. Credit check
 - d. Criminal background check
4. New York University *workforce members* who access *EPHI* will sign *confidentiality* agreements in which they agree not to provide *EPHI* to or to discuss confidential information with unauthorized persons. The appropriate Human Resources personnel will develop a system for retaining such signed agreements.

5. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: ADDRESSABLE Implementation Specification for Workforce Security Standard

HIPAA HEADING: Workforce Clearance Procedure

REFERENCE: 45 CFR 164.308(a)(3)(ii)(B)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement procedures to determine that the access of a workforce member to Electronic Protected Health Information (EPHI) is appropriate.”

4.C Termination Procedures

1. Each *covered component* of New York University will implement a documented process for terminating access to *EPHI* when the employment of *workforce members* ends or access is no longer appropriate as set forth in New York University’s ***Workforce Clearance Procedure operational specification*** (see 4.B), ***Information Access Management policy*** (HIPAA Policy 5) and ***Access Establishment and Modification operational specification*** (see 5.B), for example due to a change in position such that the *workforce member* no longer requires access to *EPHI*.
2. When a *workforce member* provides notice of his or her intention to end employment at New York University, the affected Human Resources department and the *workforce member’s* supervisor shall give reasonable notice to the persons responsible for terminating access to the *EPHI* for the departing *workforce member* so that access can be terminated when s/he leaves.
3. Each *covered component* shall log, track, and securely maintain receipts and responses to such termination of access notices, including the following information:
 - a. Date and time of notice of *workforce member* departure received
 - b. Date of planned *workforce member* departure
 - c. Description of access to be terminated
 - d. Date, time, and description of actions taken
4. When *workforce members* end employment with New York University, all privileges to access *EPHI* Systems, including both internal and remote *information system* privileges, shall be disabled or removed by the time of departure, or if not feasible, as soon thereafter as possible. When New York University *workforce members* need to be terminated immediately, New York University and/or the covered component shall remove or disable their *information system* privileges before they are notified of the termination, when feasible. *Information system* privileges include

workstations and server access, data access, network access, email accounts, and inclusion on group email lists.

5. Physical access to areas where *EPHI* is located shall be terminated as appropriate. New York University will be alert to situations where *workforce members* are terminated and may pose risks to the security of *EPHI*.
6. New York University *workforce members* shall have their *EPHI information system* privileges disabled after their access methods or user IDs have been inactive for a period of inactivity to be determined by the *EPHI* security officer at the covered component. New York University shall review privileges that are disabled due to inactivity and take the necessary steps to determine the cause of the inactivity. If inactivity is due to termination of employment, New York University will promptly terminate all *information system* privileges and notify appropriate New York University personnel to terminate physical access to areas where *EPHI* is located. If inactivity is due to other causes, New York University shall complete a review and take measures to terminate, limit, suspend, or maintain the *workforce member's* access, as appropriate.
7. Each *covered component* shall ensure that cryptographic keys are available to the appropriate managers or administrators if departing *workforce members* have used *cryptography* on *EPHI*.
8. A *workforce member* who ends employment with New York University shall not retain, give away, or remove from New York University premises any *EPHI*. At the time of his or her departure, a *workforce member* shall provide *EPHI* in his or her possession to his or her supervisor. New York University reserves the right to pursue any and all remedies against *workforce members* who violate this provision. Departing *workforce members'* supervisors shall determine the appropriate handling of any *EPHI* that departing *workforce members* possess, in accordance with the ***Device and Media Controls policy*** (HIPAA Policy 14).
9. New York University shall deactivate or change physical security access codes used to protect *EPHI* Systems of departing *workforce members*, when known.
10. Each *covered component* of New York University will implement a documented procedure for return to New York University at the time of departure supplied equipment and property that contains or allows access to *EPHI*, and will disable and remove, by the time of, or if not feasible, immediately after, the *workforce member's* departure, access to *EPHI* Systems held by the *workforce member*. Each *covered component* shall track and log the return of such equipment and property with the *workforce member's* name, date and time equipment and property was returned, and identification of returned items, and shall securely maintain the tracking and logging information. The equipment and property that may contain, or allow or enable the *workforce member* to access, *EPHI* include:
 - a. Portable computers
 - b. Personal Digital Assistants (PDAs)
 - c. Name tags or name identification badges
 - d. Security tokens
 - e. Access Cards
 - f. Building, desk, or office keys

11. HIPAA REGULATORY INFORMATION

CATEGORY: Administrative Safeguards

TYPE: ADDRESSABLE Implementation Specification for Workforce Security Standard

HIPAA HEADING: Termination Procedures

REFERENCE: 45 CFR 164.308(a)(3)(ii)(C)

SECURITY REGULATION IMPLEMENTATION SPECIFICATION LANGUAGE:

“Implement procedures for terminating access to electronic protected health information when the

employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedure] of this section.”

DEFINITIONS

Availability

Confidentiality

Covered component

Cryptography

Electronic Protected Health Information (or EPHI)

EPHI systems

HIPAA Security Regulations

Information system

Integrity

Workforce member

RELATED HIPAA DOCUMENTS

HIPAA Policy 1 – Overview: Policies, Procedures, and Documentation

HIPAA Policy 5 - Information Access Management

HIPAA Operational Specification 5.A - Access Authorization

HIPAA Operational Specification 5.B - Access Establishment and Modification

HIPAA Policy 10– Business Associate Contracts and Other Arrangements

HIPAA Policy 11 - Facility Access Controls

HIPAA Operational Specification 11.C - Access Control and Validation Procedures

HIPAA Privacy Regulations covered component’s Minimum Necessary Policy

Public Law 104-191, August 21, 1996, Health Insurance Portability and Accountability Act of 1996, <<http://aspe.os.dhhs.gov/admsimp/pl104191.htm>>.

Part II, Department of Health and Human Services, 45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule, February 20, 2003, <<http://aspe.hhs.gov/admsimp/FINAL/FR03-8334.pdf>>.